Mapping the Risks

Assessing the Homeland Security Implications of Publicly Available Geospatial Information

JOHN C. BAKER, BETH E. LACHMAN, DAVID R. FRELINGER, KEVIN M. O'CONNELL, ALEXANDER C. HOU, MICHAEL S. TSENG, DAVID ORLETSKY, CHARLES YOST

Rand National Defense Research Institute

Summary by Larry Stout
May 8, 2004

5. Key Findings and Recommendations

a. Demand Side

i. Attackers have substantial flexibility in fulfilling their information needs for attacking U.S. homeland locations.

ii. As opportunistic attackers, terrorists usually possess the advantage of having access to diverse sources for meeting their mission critical information needs, as well as the freedom to adjust the attack to meet the amount of information available.

b. Supply Side

i. Our federal geospatial information survey found that publicly available geospatial information is spread across a wide range of federal government agencies and offices.

ii. Our analysis found that very few of the publicly accessible federal geospatial sources appear useful to meeting a potential attacker's information needs.

iii. Our analysis also suggests that most publicly accessible federal geospatial information is unlikely to provide significant (i.e., both useful and unique) information for satisfying attackers' information needs.

iv. In many cases, diverse alternative geospatial and nongeospatial information sources exist for meeting the information needs of potential attackers.

c. Broader Implications

i. The ability of potential attackers to exploit publicly available geospatial information significantly varies with the type of information needed.

ii. Our results do not rule out the possibility that federal publicly available geospatial information could be exploited by potential attackers, including the possibility that discrete pieces of publicly accessible geospatial information could be aggregated by the attacker with the aim of achieving greater targeting value than is apparent when the information is viewed separately.

iii. Decisions about whether and how to restrict geospatial information would benefit from applying an analytic framework to help assess the sensitivity of a piece of geospatial information being publicly available and the security benefits and societal costs of restricting public access.

iv.. Assessing the societal benefits and costs of restricting public access to geospatial information is not straightforward.

d. General Recommendations

i. The federal government has a unique role in providing geospatial guidance to federal agencies, as well as insights on information sensitivity for nonfederal organizations.

ii. The main recommendation of this report is that the federal government play a proactive role in bringing greater coherence and consistency to the question of assessing the homeland security implications of publicly available geospatial information.

iii. The federal government can increase the awareness of the public and private sectors concerning the potential sensitivity of geospatial information.

xii. The federal government can increase the awareness of the public and private sectors concerning the potential sensitivity of geospatial information.

iv. An analytical process should be used by federal agencies and other organizations to assess the potential homeland security sensitivity of specific pieces of geospatial information that is publicly available and whether restricting access would enhance security.

v. For the longer term, the federal government should develop a more comprehensive model for addressing the security of geospatial information.